

## Title of Tutorial: Surviving the FIPS 140-1 Validation Process

Tom Caddy,  
Brenda Kallighan,  
Patricia Lareau,  
InfoGard Laboratories Inc.

The Cryptographic Module Validation Program, which tests cryptographic modules to the FIPS 140-1 and other cryptography based standards, began in 1995. Since that time, the program has validated in excess of 50 modules and has proved itself to be a valuable contributor to the security metrics and level of assurance required by decision makers when procuring equipment where cryptographic functionality is a component.

This tutorial brings to the attendees InfoGard Laboratories' experience as the first certified NVLAP laboratory in conducting Cryptographic Module Validations at all 4 levels and 3 embodiments including software applications. It is our goal to introduce the subject and discuss the process from both a business and a technical perspective.

A successful evaluation begins with a clear understanding of your own business goals, the role the lab plays, and the objectives that motivate the NIST program. We will discuss the components of a strategy that make the process a successful one, achieving both 140-1 compliance as well as your specific business objectives.

### Business Strategies:

- What business strategies are enhanced by obtaining a NIST validation for your product? What level of validation is appropriate?
- Planning for a FIPS 140-1 validation:
  - When validation can occur concurrently with design
  - When the design or product already exists
  - Scheduling and resource planning
  - Tradeoffs and Decisions
- Selecting a NVLAP Laboratory that meets your needs
- How will the FIPS 140-2 affect my strategy?

### Technical Objectives:

- FIPS 140-1 Requirements
  - How to ensure a product meets the overall intent of your design and still meet FIPS 140-1 requirements
- Validation Process
  - An overview of the validation process, from documentation requirements to report submittal and review by NIST.
  - What role the Laboratory plays in the process
  - What role the Vendor plays in the process
- Revalidation – What constitutes a revalidation and what processes to follow